

RICHMOND POLICE DEPARTMENT



11-13

FINANCIAL AND TECHNOLOGY CRIMES UNIT OPERATING MANUAL

Rodney D. Mance

Chief of Police or Designee

4/24/2008

Table of Contents

I. Purpose	3
II. Responsibility.....	3
III. Hours.....	3
IV. Procedure.....	3
V. Metro Richmond Identity Theft Task Force.....	4
VI. Evidence Collection.....	5
VII. Reports.....	5
VIII. Specialized Equipment.....	5
IX. Specialized Training / Certifications.....	6

PURPOSE

The purpose of this manual is to establish an operational procedure for the Financial and Technology Crimes Unit.

RESPONSIBILITY

The Financial and Technology Crimes Unit consists of four Richmond Police Department Detectives and a Sergeant. One Detective is assigned full time to the Metro Richmond Identity Theft Task Force which operates out of the US Postal Inspection Services Richmond Field Office. It is the Financial and Technology Crimes Unit's responsibility to investigate all reports of large embezzlement, fraud, and other financial transactions where criminal conduct has occurred. Simple check fraud cases will remain with the Precinct Detectives. This unit also conducts all seizure and analysis of computer and digital evidence. One Detective is responsible for this function in a full time capacity. In addition two Detectives investigate online child pornography on a part-time basis.

HOURS

The normal working hours of the Police Detectives assigned to the Financial and Technology Crimes Unit are 0800 hours to 1630 hours, Monday through Friday. These hours are subject to change based upon the needs of the Unit with approval through proper channels.

PROCEDURE

The Financial and Technology Crimes Unit receives cases from a variety of sources. Many complaints are referred to the Unit from the Commonwealth Attorney's Office, financial institutions, telephone calls and IBRs taken by patrol officers. The Sergeant will review each complaint and assign it to one of the detectives. The Sergeant will also work cases when the volume is high. Cases investigated by the Detective assigned to the Metro Richmond Identity Theft Task Force may not pass through the Unit and are routinely assigned by the Task Force Supervisor. Cases may be referred to the Task Force after proper approval is made by the Sergeant and is determined to meet guidelines adopted by the Task Force.

The Sergeant, with the assistance of the Commonwealth's Attorney, will determine jurisdiction on matters that may involve multi jurisdictional crimes. For instance, an on-line fraud may be prosecuted in two different jurisdictions to include a location out of state. Each investigation will be handled on a case by case basis to determine which location is better suited for a successful prosecution. Ultimately however, the final decision rests with the Office of the Commonwealth Attorney.

Any incident that is reported into the IBR system is automatically referred if the loss is greater than \$15,000.00. Often, the Richmond Commonwealth Attorney's Office refers cases of fraud

and/or embezzlement to the Unit, after the incident has been brought to their attention by the victim, the victim's attorney or other representative. Crime victims are also identified by referrals from banks and financial institutions. Identified crime victims will be updated with relevant information regarding the status of their case.

METRO RICHMOND IDENTITY THEFT TASK FORCE

The mission of the Metro Richmond Identity Theft Task Force is to protect the citizens of the Metro Richmond, VA area from identity theft related frauds and schemes, through a cooperative effort by local, state, and federal law enforcement agencies and prosecutors. In October of 2004, the Metro Richmond Identity Theft Task Force was formed to develop a cooperative effort with various federal, state, and local law enforcement agencies, to address the growing problem of financial fraud and identity theft crimes.

The Metro Richmond Identity Theft Task Force has been charged with the investigation and prosecution of criminal offenses involving advance fee and split-deposit schemes, counterfeit checks, internet fraud, stolen government checks, identity thefts and identity take-overs within the Richmond Metropolitan area placing an emphasis on organized activity. The task force is committed to aggressively investigating and prosecuting offenders, of these financial crimes, in state and federal courts.

The core members of the Metro Richmond Identity Theft Task Force are representatives from the U.S. Postal Inspection Service, Chesterfield County Police Department, FBI, Henrico County Bureau of Police, Richmond Police Department, U.S. Secret Service, U.S. Attorney's Office-Eastern District of Virginia, Virginia Attorney General's office. The participating members include the Diplomatic Security Office, Petersburg Police Department, U.S. Department of Defense, U.S. Department of Housing and Urban Development, U.S. Social Security Administration, Better Business Bureau and the National White Collar Crime Center.

The Metro Richmond Identity Theft Task Force assists victims and potential victims in several ways. The website, <http://www.richmondidtheft.com/>, provides the following information:

- Procedures to identify when a crime has occurred
- Procedures to report identity theft crimes
- Instructions for filing a complaint
- Action steps for victims once a crime has been identified
- Telephone numbers, addresses and email addresses to contact the Task Force directly
- Links to victim resources websites
- Prevention tips
- Related state and federal laws
- Updated scam alerts
- Press releases and news
- Most Wanted page

COLLECTION OF EVIDENCE

Evidence used to build a case will be collected utilizing standard investigative techniques including but not limited to:

- Interviews
- Grand Jury Subpoenas
- Search Warrants
- Surveillance
- Informants

A detailed analysis of bank and/or business records may be required to properly trace the flow of illegally obtained funds in order to determine whether a criminal violation has occurred. This may include assistance from the National White Collar Crime Center (NW3C), a federally funded agency that can provide expert testimony, spreadsheets, charts and other resources that can assist the Detective at trial.

The FCU shall follow procedures set forth in General Order 7-27, Computer Forensics Procedures when collecting any form of digital evidence.

REPORTS

The Detective will complete an IBR once jurisdiction within the City of Richmond has been established. The IBR may also be completed by a uniformed Richmond police officer on the scene. The IBR shall be reviewed and approved by a Police Department supervisor immediately (or prior to completion of the tour) and forwarded through proper channels.

Detectives will also complete an Investigative Summary on any arrest and/or incident involving any unusual or extraordinary events. This could be where the loss is extraordinarily high, victim or suspect is a public figure, or any other incident that may generate a response from the media.

SPECIALIZED EQUIPMENT

The FCU maintains the following equipment:

1. FRED (Forensic Recovery of Evidence Device) – Forensic analysis computer
2. FRED SR (Forensic Recovery of Evidence Device Sr.) – Forensic analysis computer
3. MacBook Pro – Mac laptop computer used for mobile forensics and imaging
4. Cellebrite – Cell phone analysis tool
5. DataPilot – Cell phone analysis tool
6. Device Seizure – Cell phone analysis tool
7. Project-a-Phone – Cell phone analysis tool

SPECIALIZED TRAINING / CERTIFICATIONS

The FCU detective assigned to Computer Forensics is required to maintain the following certifications:

- **CFCE – Certified Forensic Computer Examiner (IACIS)**
- **A+ Certified Professional**
- **Network+ Certified Professional**

Specialized training for detectives assigned to the FCU is available through the National White Collar Crimes Center (NW3C). This training is usually conducted at little to no cost to the Department and is provided to detectives as often as Department funding will permit.